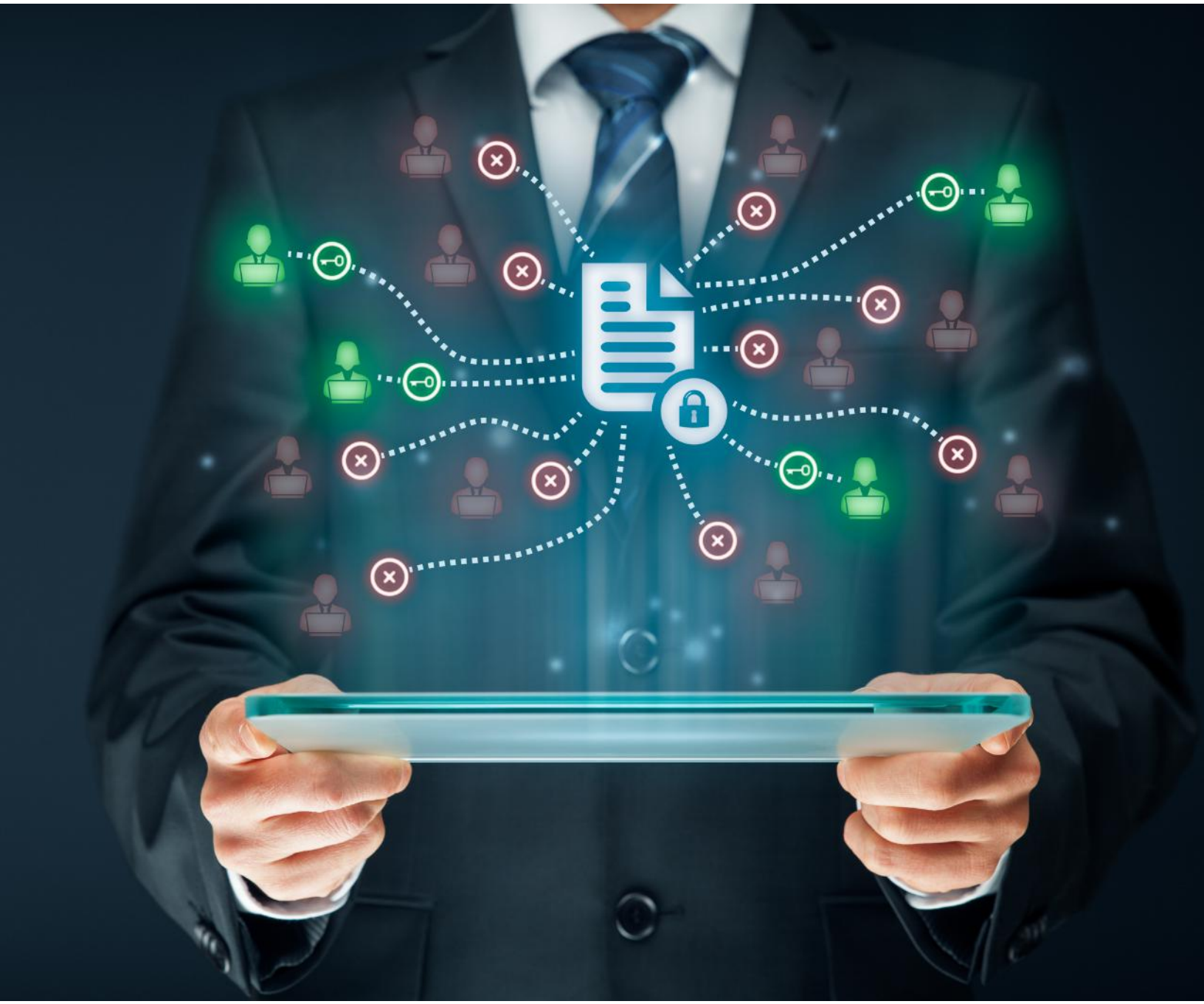
Security Awareness Training



Security Awareness Training:

Purpose

- To provide a brief overview of some current security issues.
- To increase awareness of security vulnerabilities in our everyday business and personal practices.
- To reduce the risk of security issues within the company.
- To satisfy annual training requirements.

Danger with Email Attachments

Email attachments are a common attack vector

Email is easily circulated – Forwarding email is so simple that viruses can quickly infect many machines. Most malware don't even require users to forward the email—they scan a users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.

Almost any type of file can be attached to an email message, so attackers have more freedom with the types of malware they can send.

Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any malware within the attachments.

Steps to Protect Yourself

1. Be wary of unsolicited attachments, even from people you know – Just because an email message looks like it came from your mom, grandma, or boss doesn't mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes email messages that appear to be from your ISP or software vendor and claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.

2. Keep software up to date – Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

3. Turn off the option to automatically download attachments. Many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.

4. Trust your instincts – If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the anti-virus software might not have the signature. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.

5. Save and scan any attachments before opening them - If you have to open an attachment before you can verify the source, take the following steps:
- Be sure your anti-virus software is up to date.
- Save the file to your computer or a disk.
- Manually scan the file using your anti-virus software.
- If the file is clean and doesn't seem suspicious, go ahead and open it.

6. Consider creating separate accounts on your computer – Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.

Ransomware

What is Ransomware?

Ransomware is a malicious program that locks or encrypts hard drives. The victim is told that they must paid a fee for the key to unlock/decrypt their files.

Why is Ransomware different?

Ransomware didn't even comprise 1% of all Windows malware in 2016, rendering it a "marginal phenomenon" despite causing mass disruption.

However, this class of malware doesn't need to be distributed en masse like traditional viruses, instead of using "highly-complex, state-of-the-art encryption protocols", "sophisticated server infrastructure" for key generation and management, and a targeted approach for maximum effect.

Ransomware tends to seek its victims in a targeted business environment. For instance, emails infected with ransomware are sent out almost exclusively on weekdays. Public sector organizations, healthcare, and retail were some of the most popular targets for ransomware authors.

Half of organizations hit by a ransomware attack are struck multiple times, with exposed infrastructure stretching well beyond the endpoint.

Although unsolicited emails are often the cause of initial infection, exploiting employees' lack of cyber-savvy, and infecting endpoints (60%), a third (33%) of attacks struck corporate servers and 7% targeted cloud apps.

Elsewhere there was relatively good news for Microsoft, as the overall volume of Windows malware encountered by virus catchers fell by 15% from 2015 to 2016, while macOS and Linux malware both tripled and Android malware doubled. The bad news continued for Apple with Q1 2017 figures confirming macOS malware doubled in the first four months of the year.

Avoiding Social Engineering and Phishing Attacks

What is social engineering?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, they may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, they may contact another source within the same organization and rely on the information from the first source to add to their credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- Holidays

How to avoid being a victim?

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send sensitive information over the Internet before checking a website's security.

Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.

Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

Take advantage of any anti-phishing features offered by your email client and web browser.

Reducing the Risk of SNMP Abuse

The Simple Network Management Protocol (SNMP) may be abused to gain unauthorized access to network devices.

SNMP depends on secure strings (or "community strings") that grant access to portions of devices' management planes.

SNMPv3 should be the only version of SNMP employed because SNMPv3 has the ability to authenticate and encrypt payloads. When either SNMPv1 or SNMPv2 are employed, an adversary could sniff network traffic to determine the community string. This compromise could enable a man-in-the-middle or replay attack.

Configure SNMPv3 to use the highest level of security available on the device; this would be *authPriv* on most devices. *authPriv* includes authentication and encryption features, and employing both features enhances overall network security.

Segregate SNMP traffic onto a separate management network. Management network traffic should be out-of-band; however, if device management must coincide with standard network activity, all communication occurring over that network should use some encryption capability. If the network device has a dedicated management port, it should be the sole link for services like SNMP, Secure Shell (SSH), etc.

Ensure administrative credentials are properly configured with different passwords for authentication and encryption. In configuring accounts, follow the principle of least privilege. Role separation between polling/receiving traps (reading) and configuring users or groups (writing) is imperative because many SNMP managers require login credentials to be stored on disk in order to receive traps.

References

Email Attachments

https://www.us-cert.gov/ncas/tips/ST04-010

Ransomware

https://www.infosecurity-magazine.com/news/half-of-ransomware-victims-are-hit
https://www.infosecurity-magazine.com/news/av-test-ransomware-is-a-marginal

Social Engineering

https://www.us-cert.gov/ncas/tips/ST04-014

SNMP Abuse

https://www.us-cert.gov/ncas/alerts/TA17-156A